ISO27001内部監査チェックリスト（附属書A管理策）

記入者	確認（承認）

監査該当部門は、●で示しています。総合評価結果は適合、不適合、観察事項とします。－は非該当もしくは今回の監査では確認しなかった事項です。
なお、有効性評価については、管理策の目的を満たしているか、結果は出ているかを評価し、○、△、×で評価します。

規格項目	チェック内容	IS管理責任者	営業部門	技術部門	総務部門	コメント	有効性評価	総合評価結果	備考
A.5 情報セキュリティのための方針群 A.5.1 情報セキュリティのための経営陣の方向性 目的:情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項、関連する法令及び規制に従って、規定するため。									
A.5.1.1 情報セキュリティのための方針群	「情報セキュリティ基本方針」を始めとする方針群を社長の承認を得て、発行し、全従業員及び関連する外部関係者に公表し、通知しているか	●							A.6.2.1、A.6.2.2、A.9.1.1、A.9.1.2、A.10.1.1、A.10.1.2、A.11.2.9、A.12.3.1、A.13.2.1、A.14.2.1、A.15.1.1、A.18.1.4
A.5.1.2 情報セキュリティのための方針群のレビュー	レビュー実施のための手順は確立されているか	●							
A.6 情報セキュリティのための組織 A.6.1 内部組織 目的:組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。									
A.6.1.1 情報セキュリティの役割及び責任	情報セキュリティの責任を文書化して、具体的に明確にしてるか	●							
A.6.1.2 職務の分離	不正使用の危険性を低減するために、職務を分離させるか、一つの職務権限に一人ではなく、複数の者を割り当てているか	●							
A.6.1.3 関係当局との連絡	具体的な連絡体制を確立しているか	●							
A.6.1.4 専門組織との連絡	具体的な連絡体制を確立しているか	●							
A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ	プロジェクトマネジメントにおいても情報セキュリティの取り組みを行っているか	●							
A.6.2 モバイル機器及びテレワーキング 目的:モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。									
A.6.2.1 モバイル機器の方針	モバイル機器の利用を行う場合の方針は定めているか	●							
A.6.2.2 テレワーキング	テレワーキングを行う場合のセキュリティ対策は定めているか	●							
A.7 人的資源のセキュリティ A.7.1 雇用前 目的:従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。									
A.7.1.1 選考	採用予定者が、情報セキュリティに関する必要な力量を備えていることの確認を行っているか				●				
A.7.1.2 雇用条件	採用予定者に対して、「機密保持誓約書」に署名、提出させているか				●				
A.7.2 雇用期間中 目的:従業員及び契約相手が情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするた									
A.7.2.1 経営陣の責任	すべての従業員及び契約相手に、当社の方針及び手順に従ったセキュリティの適用を要求しているか	●							
A.7.2.2 情報セキュリティの意識向上、教育及び訓練	すべての従業員及に、自覚教育を実施しているか	●							
A.7.2.3 懲戒手続	情報セキュリティ違反を犯した従業員に対して、懲戒規定に則り処罰しているか	●			●				
A.7.3 雇用の終了又は変更 目的:雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。									
A.7.3.1 雇用の終了又は変更に関する責任	すべての従業員に対して、雇用の終了又は変更の実施に対する責任及び義務をを明確に定め、その対応を確実に行っているか				●				
A.8 資産の管理 A.8.1 資産に対する責任 目的:組織の資産を特定し、適切な保護の責任を定めるため。									
A.8.1.1 資産目録	適用範囲内における情報資産は、「情報資産台帳」において特定しているか		●	●	●				
A.8.1.2 資産の管理責任	資産の管理責任者は、「情報資産台帳」にて明示しているか		●	●	●				
A.8.1.3 資産利用の許容範囲	資産利用の許容範囲は、「情報資産台帳」にて明示しているか		●	●	●				
A.8.1.4 資産の返却	雇用、契約の終了時に、該当する従業員又は外部利用者から、社員証、社用名刺、施設入退室カード、貸与PC、携帯電話をはじめ、貸与した情報資産の返却を確実に行っているか		●	●	●				
A.8.2 情報分類 目的:情報に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。									
A.8.2.1 情報の分類	情報の分類は、基準に基づき、分類しているか		●	●	●				
A.8.2.2 情報のラベル付け	情報のラベル付けは、実施しているか		●	●	●				
A.8.2.3 資産の取扱い	資産の取扱いは、分類に従って適切に行っているか		●	●	●				
A.8.3 媒体の取扱い 目的:媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。									
A.8.3.1 取外し可能な媒体の管理	USB等、携帯可能な記録媒体のネットワークへの接続と使用は行っていないか		●	●	●				
A.8.3.2 媒体の処分	不要になった媒体は、速やかにかつセキュリティを保って処分しているか		●	●	●				
A.8.3.3 物理的媒体の輸送	重要な書類や媒体を宅配便で送付する場合は、信頼できる業者に委託しているか		●	●	●				
A.9 アクセス制御 A.9.1 アクセス制御に対する業務上の要求事項 目的:情報及び情報処理施設へのアクセスを制御するため。									
A.9.1.1 アクセス制御方針	アクセス制御方針を定め、周知しているか	●							
A.9.1.2 ネットワーク及びネットワークサービスへのアクセス	社内のネットワーク及びネットワークサービスへのアクセスは、セキュリティが保たれているか		●	●	●				
A.9.2 利用者アクセスの管理 目的: システム及びサービスへの認可された利用者のアクセスを確実にし、認可されていないアクセスを防止す									

規格項目	チェック内容	IS管理責任者	営業部門	技術部門	総務部門	コメント	有効性評価	総合評価結果	備考
A.9.2.1 利用者登録及び登録削除	社内システムへの利用者登録及び登録削除は適切に行っているか			●	●				
A.9.2.2 利用者アクセスの提供	情報システム責任者は、すべてのシステムにおいて、ISMS管理責任者の承認を得て、個人ごとにIDとパスワードを発行しているか			●					
A.9.2.3 特権的アクセス権の管理	管理者権限の割当ては最小限とし、割当て者には責任を認識させ、厳重な管理を誓約させているか			●					
A.9.2.4 利用者の秘密認証情報の管理	パスワードの新規発行、更新をする場合、事前に、利用者の本人確認を行っているか			●					
A.9.2.5 利用者のアクセス権のレビュー	定期的(1回/年)に、アカウントリストの見直しを行い、適切であるか、抹消漏れがないかを確認しているか			●					
A.9.2.6 アクセス権の削除又は修正	雇用、契約の終了時に、情報システム責任者に依頼して、該当する従業員の社内システムへのアクセス権限をすべて抹消しているか			●	●				
A.9.3 利用者の責任 目的:利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。									
A.9.3.1 秘密認証情報の利用	パスワードは、8文字以上でアルファベットと数字を混在させるなどしているか	●		●					
A.9.4 システム及びアプリケーションのアクセス制御 目的:システム及びアプリケーションへの、認可されていないアクセスを防止するため。									
A.9.4.1 情報へのアクセス制限	認可された者だけがアクセスできるようなシステム及び業務用ソフトウェアは、適切に管理を行っているか			●					
A.9.4.2 セキュリティに配慮したログオン手順	許容失敗回数の制限や入力したパスワードは、マスキングして隠すなどセキュリティに配慮したログオン手順になっているか			●					
A.9.4.3 パスワード管理システム	利用者がパスワードを再設定する場合、文字数が8桁未満は受け付けないなど、設定ルールは機能しているか			●					
A.9.4.4 特権的なユーティリティプログラムの使用	OSや業務用ソフトウェアをチューニングにしたりするユーティリティソフトの使用を禁止しているか			●					
A.9.4.5 プログラムソースコードへのアクセス制御	プログラムソースコードへのアクセス管理は行っているか			●					
A.10 暗号 A.10.1 暗号による管理策 目的:情報の機密性、真正性または完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。									
A.10.1.1 暗号による管理策の利用方針	暗号の利用方針を定め、周知しているか			●					
A.10.1.2 鍵管理	暗号に使用する鍵は、適切に管理を行っているか			●					
A.11 物理的及び環境的セキュリティ A.11.1 セキュリティを保つべき領域 目的:組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため									
A.11.1.1 物理的セキュリティ境界	セキュリティエリアのルールは周知され、守られているか		●	●	●				
A.11.1.2 物理的入退管理策	物理的入退管理のルールは周知され、守られているか		●	●	●				
A.11.1.3 オフィス、部屋及び施設のセキュリティ	当該建物・部屋に具備するべき物理的セキュリティは適切か	●							
A.11.1.4 外部及び環境の脅威からの保護	外部訪問者からのぞき見、盗み聞きされないような、適切な作業環境になっているか	●							
A.11.1.5 セキュリティを保つべき領域での作業	「入退室管理台帳」は適切に運用されているか		●	●	●				
A.11.1.6 受渡場所	宅配便などの外部者との受渡場所は設定したセキュリティエリアで実施しているか		●	●	●				
A.11.2 装置 目的:資産の損失、損傷、盗難又は劣化、及び組織の活動に対する妨害を防止するため。									
A.11.2.1 装置の設置及び保護	サーバーなどの重要な装置は許可されていない者による悪用を防止できる環境に設置してあるか			●					
A.11.2.2 サポートユーティリティ	停電、その他の故障から保護するために、サーバーには、UPS(無停電電源装置)を設置し、適切に維持管理されているか			●					
A.11.2.3 ケーブル配線のセキュリティ	通信ケーブル及び電源ケーブルは、傍受又は損傷から保護し、適切に収納されているか			●					
A.11.2.4 装置の保守	PCやサーバー、ネットワーク機器などの装置の保守は適切か			●	●				
A.11.2.5 資産の移動	ノートPC等の装置の移動(持ち出し)は、管理者の承認を得て、行っているか		●	●	●				
A.11.2.6 構外にある装置及び資産のセキュリティ	自社外(移動先、顧客先など)にあるノートPC及び情報資産に対しては、セキュリティリスクを考慮して、作業を行っているか		●	●	●				
A.11.2.7 装置のセキュリティを保った処分又は再使用	パソコン等の装置の処分又は再利用に際して、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去しているか			●	●				
A.11.2.8 無人状態にある利用者装置	利用者は、外出時、帰宅時は必ずPC電源をシャットダウンしているか		●	●	●				
A.11.2.9 クリアデスク・クリアスクリーン方針	利用者は、外出時、離席時、帰宅時において、重要な情報(媒体含む)を机上に放置していないか、離席時は、適切なロック機能(パスワードによって保護されたスクリーンセーバ等)の利用を実施しているか		●	●	●				
A.12 運用のセキュリティ A.12.1 運用の手順及び責任 目的:情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため。									
A.12.1.1 操作手順書	必要に応じて、操作の手順書(取扱説明書)を整備し、必要とするすべての利用者に対して利用可能であるか	●		●					
A.12.1.2 変更管理	情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、情報セキュリティ委員会での審議を経て、経営陣の承認を得て実施しているか	●		●					
A.12.1.3 容量・能力の管理	システムの容量・能力の管理及びその予測を行っているか			●					
A.12.1.4 開発施設、試験施設及び運用施設の分離	開発環境は、分離しているか			●					
A.12.2 マルウェアからの保護 目的:情報及び情報処理施設がマルウェアから保護されることを確実にするため。									
A.12.2.1 マルウェアに対する管理策	個人貸与PCのウィルス対策機能が有効となっているか、パターン定義ファイルが最新のものになっているか		●	●	●				
A.12.3 バックアップ 目的:データの消失から保護するため。									

規格項目	チェック内容	IS管理責任者	営業部門	技術部門	総務部門	コメント	有効性評価	総合評価結果	備考
A.12.3.1 情報のバックアップ	重要な情報のバックアップ方法はルール化され、確実に行っているか		●	●	●				
A.12.4 ログ取得及び監視 目的:イベントを記録し、証拠を作成するため。									
A.12.4.1 イベントログ取得	ネットワーク機器や業務システムについて、ログ採取の是非、保存期間を決定しているか			●					
A.12.4.2 ログ情報の保護	採取したログを、改ざん及び認可されていないアクセスから保護しているか			●					
A.12.4.3 実務管理者及び運用担当者の作業ログ	作業を行った運用記録(作業日報)を作成し、定期的にレビューを行っているか			●					
A.12.4.4 クロックの同期	NTPサーバーを利用して、自社内のすべての情報処理システムのクロックの同期を図るようにしているか			●					
A.12.5 運用ソフトウェアの管理 目的:運用システムの完全性を確実にするため。									
A.12.5.1 運用システムに関わるソフトウェアの導入	運用中の情報システムにおけるソフトウェア及びプログラムライブラリーの更新は、適切な管理層の許可に基づき、訓練された実務管理者だけが行っているか			●					
A.12.6 技術的ぜい弱性の管理 目的:技術的ぜい弱性の悪用を防止するため。									
A.12.6.1 技術的ぜい弱性の管理	常に業務用ソフトウェアのベンダーや、外部の専門機関が発する情報を、時機を失せずに取得し、自らが管理するシステムのぜい弱性の改善を行っているか			●					
A.12.6.2 ソフトウェアのインストール制限	許可していないソフトウェアのインストールの監視を行っているか			●					
A.12.7 情報システムの監査に対する考慮事項 目的:運用システムに対する監査活動の影響を最小限にするため。									
A.12.7.1 情報システムの監査に対する管理策	運用システムの点検を伴う監査要求事項及び活動は、業務プロセスの中断のリスクを最小限に抑えるために、慎重に計画し、実行しているか			●					
A.13 通信のセキュリティ A.13.1 ネットワークセキュリティ管理 目的:ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。									
A.13.1.1 ネットワーク管理策	自社のネットワークについて、適切な分離、無線データの暗号化、適切なログ取得及び監視など、行うべき項目は確実に行っているか			●					
A.13.1.2 ネットワークサービスのセキュリティ	ネットワークサービスの監視は行っているか			●					
A.13.1.3 ネットワークの分離	組織の単位や信頼性のレベル(公開されている領域やサーバー領域)等のグループごとに分離しているか			●					
A.13.2 情報の転送 目的:組織の内部及び外部に転送した情報セキュリティを維持するため。									
A.13.2.1 情報転送の方針及び手順	情報転送の方針及び手順は周知され、適切に実施されているか		●	●	●				
A.13.2.2 情報転送に関する合意	他組織と機密情報を転送する場合は、秘密保持契約等を締結し、合意しているか		●	●	●				
A.13.2.3 電子的メッセージ通信	電子メールはウィルス感染対策を施しているか、また、その利用手順は周知され、適切に実施されているか		●	●	●				
A.13.2.4 秘密保持契約又は守秘義務契約	秘密保持契約又は守秘義務契約において、その内容をレビューしているか		●	●	●				
A.14 システムの取得、開発及び保守 A.14.1 情報システムのセキュリティ要求事項 目的:ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。									
A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	情報セキュリティ要求事項の分析及び必要な要求事項の明確化を行っているか			●					
A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	不特定多数の人が利用するネットワーク(公衆ネットワーク)を利用する場合には、セキュリティ確保を確実にして利用を行っているか			●					
A.14.1.3 アプリケーションサービスのトランザクションの保護	利用するオンライン取引に含まれる情報は、通信経路の暗号化(SSL)等によって保護しているか			●					
A.14.2 開発及びサポートプロセスにおけるセキュリティ 目的:情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。									
A.14.2.1 セキュリティに配慮した開発のための方針	セキュリティに配慮した開発のための方針は策定し、関係者に周知されているか			●					
A.14.2.2 システムの変更管理手順	情報システムの変更に際しては、変更の妥当性の検証を行い、変更に関する記録を残しているか			●					
A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	オペレーティングシステムを含むプラットフォーム(情報システムの基盤)の変更に際しては、情報の機密性、完全性、可用性を考慮し、その上で動作する業務ソフトウェアへの影響やシステム全体を検証した上で実施しているか			●					
A.14.2.4 パッケージソフトウェアの変更に対する制限	市販のソフトウェアの変更は、ベンダーが提供する修正プログラムによるものを除き、行っていないか			●					
A.14.2.5 セキュリティに配慮したシステム構築の原則	情報システム構築は、情報セキュリティの必要性とアクセスの必要性の均衡を保ちながら、実施しているか			●					
A.14.2.6 セキュリティに配慮した開発環境	セキュリティに配慮した開発環境は確立されているか			●					
A.14.2.7 外部委託による開発	外部委託によるソフトウェア開発を行う場合、セキュリティ要求事項を明確にし、外部委託業者の適切な監督、監視を行っているか			●					
A.14.2.8 システムセキュリティの試験	セキュリティ機能の試験を、確実に、開発期間中に実施できるように、適切な監督、監視を行っているか			●					
A.14.2.9 システムの受入れ試験	業務用システムの新規導入及び改訂・更新する際、適切な受入試験を行っているか			●					
A.14.3 試験データ 目的:試験に用いるデータの保護を確実にするため。									
A.14.3.1 試験データの保護	試験データは保護し、管理を行っているか			●					
A.15 供給者関係 A.15.1 供給者関係における情報セキュリティ 目的:供給者がアクセスできる組織の資産の保護を確実にするため。									
A.15.1.1 供給者関係のための情報セキュリティの方針	供給者者による組織の情報へのアクセスに関して、供給者と合意し、文書化しているか			●					
A.15.1.2 供給者との合意におけるセキュリティの取扱い	供給者(外部の業者)に委託する場合に、守秘義務等を含む契約書、または覚書を取り交わしているか			●					
A.15.1.3 ICTサプライチェーン	ICTサービス及び製品に関して、情報セキュリティが確保できるように、供給者に要求しているか			●					
A.15.2 供給者のサービス提供の管理									

規格項目	チェック内容	IS管理責任者	営業部門	技術部門	総務部門	コメント	有効性評価	総合評価結果	備考
目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。									
A.15.2.1 供給者のサービス提供の監視及びレビュー	供給者（外部）のサービスの監査を年一回、もしくは必要に応じて行い、その結果を情報セキュリティ委員会にて報告を行っているか	●	●	●	●				
A.15.2.2 供給者のサービス提供の変更に対する管理	供給者（外部）が提供するサービスに変更があった際は、リスクを再評価し、必要に応じて手順等を見直し、その結果を情報セキュリティ委員会にて報告を行っているか	●	●	●	●				
A.16　情報セキュリティインシデント管理 A.16.1 情報セキュリティインシデントの管理及びその改善 目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取り組みを確実にするため。									
A.16.1.1 責任及び手順	情報セキュリティインシデントが発生した場合の手順と責任は明確か	●							
A.16.1.2 情報セキュリティ事象の報告	社員は、セキュリティの弱点や脅威に気づいた場合、ISMS事務局へ報告しているか		●	●	●				
A.16.1.3 情報セキュリティ弱点の報告	ISMS事務局は、情報セキュリティ弱点に関する、利用者への周知を、社内回覧またはメールで行っているか	●							
A.16.1.4 情報セキュリティ事象の評価及び決定	ISMS管理責任者は、情報セキュリティ事象の評価及び決定を行い、その結果および指示事項を社内に伝達しているか	●							
A.16.1.5 情報セキュリティインシデントへの対応	情報セキュリティインシデントへの対応手順は明確か	●							
A.16.1.6 情報セキュリティインシデントからの学習	情報セキュリティインシデントから得られた情報は、再発防止のための社員教育に役立てているか	●							
A.16.1.7 証拠の収集	セキュリティインシデントの結果、法的処置がとられる可能性があると判断した場合は、記録、証拠を保全する手順があるか	●							
A.17　事業継続マネジメントにおける情報セキュリティの側面 A.17.1 情報セキュリティ継続 目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。									
A.17.1.1 情報セキュリティ継続の計画	困難な状況（災害もしくは大事故時など）においても、情報セキュリティ及び情報セキュリティマネジメントを適切に維持管理できるように、組織で行うべきことは明確か	●							
A.17.1.2 情報セキュリティ継続の実施	「事業継続計画書」を作成し、経営者の承認を得ているか	●							
A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価	「事業継続計画書」を検証し、評価しているか	●							
A.17.2 冗長性 目的：情報処理施設の可用性を確実にするため。									
A.17.2.1 情報処理施設の可用性	十分な冗長性を持って、情報処理施設の可用性を保つようにしているか	●		●					
A.18 順守 A.18.1 法的及び契約上の要求事項の順守 目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要									
A.18.1.1 適用法令及び契約上の要求事項の特定	「法的要求事項登録簿」の見直し及びその周知を図っているか	●			●				
A.18.1.2 知的財産権	著作権の侵害等、知的財産権の重要性について教育を行っているか		●	●	●				
A.18.1.3 記録の保護	ログや運用記録等、セキュリティに関係する重要な記録は消失、破壊、改ざんがないように管理しているか	●							
A.18.1.4 プライバシー及び個人を特定できる情報の保護	個人情報保護法や関連する各種ガイドライン等を順守しているか		●	●	●				
A.18.1.5 暗号化機能に対する規制	暗号機能の関連する協定、法令及び規制を認識しているか	●		●					出張で暗号化機能を有したパソコンを海外に持ち出す場合、国によって手続きは必要な場合がある
A.18.2 情報セキュリティのレビュー 目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。									
A.18.2.1 情報セキュリティの独立したレビュー	情報セキュリティのための管理目的、管理策、方針、プロセス、手順について見直しを行っているか	●							
A.18.2.2 情報セキュリティのための方針群及び標準の順守	情報セキュリティ方針及び関連する手順書の順守を達成するために、すべてのセキュリティ手順が正しく実行されて	●							
A.18.2.3 技術的順守のレビュー	情報システムが、当社の定めたセキュリティ基準に従って順守されているかどうか、定めに従って点検を行っているか			●					